12 FAM 640 DOMESTIC AND OVERSEAS AUTOMATED INFORMATION SYSTEMS CONNECTIVITY

12 FAM 641 GENERAL

(TL:DS-51; 4-12-96)

a. This subchapter provides network security requirements which build on the stand-alone systems security requirements contained in other subchapters of Chapter 600. This subchapter's requirements apply to both domestic and overseas classified and unclassified systems operating in the system-high, dedicated, or multi-level mode of operation, connected by way of network services or point-to-point communications.

b. Due to differences in hardware and software capabilities, of and between different systems, system managers must implement the controls described in this subchapter as they apply to specific systems installations.

12 FAM 641.1 Mode of Operation for Automated Information Systems

(TL:DS-51; 4-12-96)

The system manager must identify the mode of operation for each automated information system prior to joining it in a network. The system manager must also identify the mode of operation for each AIS already joined in a network at the time of this publication. See the blue pages for accepted modes of operation.

12 FAM 641.2 Level of Trust for Automated Information Systems

(TL:DS-51; 4-12-96)

In accordance with the Department of Defense's Trusted Computer System Evaluation Criteria (TCSEC), and as stated in section 12 FAM 652, specific levels of trust, i.e., hardware and software assurance measures, are required for AISs. The system manager or Departmental representative should refer to the Evaluated Products List (EPL) contained in the Information Systems Security Products and Services Catalogue for operating systems and add-on security subsystem components. These systems and subsystems have been evaluated by the National Security Agency and assigned a specific level of trust. The system manager must identify the level of trust for each AIS before joining it in a network. The system manager must also identify the level of trust for each AIS already joined in a network at the time of this publication. If the AIS currently in use is not listed in the EPL, the system manager must note this for use in section 12 FAM 641.3 .

12 FAM 641.2-1 C-2 Level of Trust for Classified AISs

(TL:DS-51; 4-12-96)

a. For classified processing in the system high and the dedicated mode, the Department requires that system and subsystem acquisition authorities select C-2 rated operating systems listed in the Evaluated Products List (EPL).

b. If the use of EPL products is not feasible, or if the product selected has not received a full evaluation from NSA, the acquisition authority must contact DS/CIS/IST. DS/CIS/IST may forego the requirement for rated products and allow system acquisition authorities to purchase the selected product after consultation with the National Security Agency's Security Profiling and Trusted Evaluation Program (TPEP) organizations.

12 FAM 641.2-2 C-2 Functionality for Unclassified Systems

(TL:DS-51; 4-12-96)

The Department does not require the use of C-2 rated operating systems listed in the Evaluated Products List for unclassified processing. However, all AISs must provide automated controlled access protection, and DS/CIS/IST recommends that C-2 rated products be used whenever possible. Operating systems must control user access to information according to "need to know" and authorization.

12 FAM 641.2-3 Security Subsystems for Microcomputers

(TL:DS-51; 4-12-96)

DS/CIS/IST has reviewed security subsystems for use by DOS-based microcomputers. In lieu of the aforementioned C-2 requirement, these subsystems meet security requirements for discretionary access control, identification and authentication, audit and object reuse. DS/CIS/IST will provide additional information upon request.

12 FAM 641.2-4 B and A Levels of Trust

(TL:DS-51; 4-12-96)

Networks operating in a multi-level mode must implement either B or A levels of trust, as defined in the Department of Defense's Trusted Computer System Evaluation Criteria.

12 FAM 641.3 Methodology for Connecting Systems Based on the Operating Mode, Level of Trust, and Classification

(TL:DS-51; 4-12-96)

The system manager will note the mode of operation, level of trust, and classification of the AISs to be connected in a network. The system manager will make network connections based upon the instructions that follow below.

12 FAM 641.3-1 Connection of Distributed Systems in a Network

(TL:DS-51; 4-12-96)

a. The Department will not require any measures to upgrade the level of trust for distributed AISs which are fielded before October 1, 1995. The system manager will connect only those systems having the same mode of operation (system-high or dedicated) and classification level.

b. After October 1, 1995 only classified AISs which have a C-2 rated operating system, or have been approved by DS/CIS/IST as having C-2 functionality for use in the system-high or dedicated mode of operation, will be fielded. The system manager will only connect newly fielded classified AISs to systems operating at the identical classification level (e.g., Secret, Confidential).

c. After October 1, 1995 only unclassified AISs that control user access to information according to “need to know” and authorization will be fielded. It is not a requirement that these AISs have a formal C-2 rating. The system manager will connect new unclassified AISs to existing systems and ensure that they operate at the identical system-high/dedicated classification level, e.g., Unclassified. As described in section 12 FAM 645, a stand-alone Department of State PC may be connected to a nongovernmental system.

12 FAM 641.3-2 Connection of PCs in a Network

(TL:DS-51; 4-12-96)

The system manager must install DS/CIS/IST-approved security subsystems on all PCs which do not have C-2 functionality. These subsystems will provide discretionary access control, identification and authentication, audit, and object reuse. PCs equipped with security subsystems may be attached to other AISs having an equivalent or greater level of trust, and will operate in the system-high or dedicated mode. PCs attached to C-2 level systems must operate at the identical classification level.

12 FAM 642 ADMINISTRATIVE SECURITY

(TL:DS-51; 4-12-96)

The following administrative security requirements apply to networks which are hierarchical, as well as networks in which all connections are equal.

12 FAM 642.1 Appointment of System Managers and Designation of Control Centers in a Hierarchical Network

(TL:DS-51; 4-12-96)

a. A network environment that encompasses systems under the control of different system managers and ISSOs must have one node within the region designated as the regional control center (RCC). This RCC must have a designated system manager to administer network operations. Administrative officers at overseas posts and/or executive directors of bureaus at domestic locations must coordinate the designation of an individual, usually one of the system managers for the connected systems, to be the RCC system manager.

b. One administrative system in the entirety of the network must have primary responsibility for managing the network. For example, the Department's unclassified network (DOSNET) and the Department's classified messaging application system (FAIS) have designated network control centers (NCCs) located at A/IM Washington. For each network, A/IM must designate an individual to be the NCC system manager (administrator for the network).

12 FAM 642.2 Appointment of ISSOs in a Hierarchical Network

(TL:DS-51; 4-12-96)

a. Administrative officers at overseas posts, and/or executive directors of bureaus at domestic locations, must coordinate the designation, in writing, of a regional ISSO. This person manages the information system security issues that extend across more than one security domain. This individual may also be the ISSO for one of the connected systems. Administrative officers or executive directors must also designate, in writing, an alternate ISSO to fulfill those responsibilities when the regional ISSO is absent.

b. A/IM is responsible for designating, in writing, an ISSO to manage the information system security issues that extend across the entire network. A/IM must also designate in writing an alternate ISSO to fulfill those responsibilities when the primary ISSO is absent.

12 FAM 642.3 Responsibilities of System Managers and ISSOs

(TL:DS-51; 4-12-96)

a. Local system managers are responsible for the operation of local networks under their control.

b. RCC system managers are responsible for the operation of regional network(s) under their control.

c. The network control center (NCC) system manager is responsible for the operation of the entire network.

d. The local information systems security officer (ISSO) is responsible for the security of all local network connections.

e. RCC ISSOs are responsible for the security of regional network(s) under their control.

f. The ISSO for the NCC is responsible for the security of Department-wide networks, e.g., DOSNET and FAIS.

g. Off-site systems and the media used on these systems must be secured in rooms equipped with DS-approved locks on doors and windows.

h. Once installed in a private or official residence, government-owned system equipment must not be moved without permission of the RSO and ISSO and must be used for official business only.

i. Only U.S. Government provided-software may be installed on off-site PCs. Privately-owned software is prohibited from being used on government owned PCs. Software must be installed by the system manager.

j. The system manager will install appropriate virus protection on all PCs prior to use since PCs installed in residences of U.S. employees are vulnerable to the threat of contamination.

k. The system manager will instruct the employee on the proper use of the anti-virus protection.

12 FAM 642.4 Management Control Process

(TL:DS-51; 4-12-96)

Unless specifically stated, the requirements that follow apply to all system managers and ISSOs.

12 FAM 642.4-1 Availability of Service

(TL:DS-51; 4-12-96)

a. System managers must establish all network operation schedules.

b. The system manager must protect telecommunication services and resources from point of origin to point of destination. This is done in accordance with the magnitude of loss or potential harm that may occur from the loss, inaccuracy, alteration, unavailability, disclosure, or misuse of transmitted information.

c. The system manager must provide for the operational availability of services according to the criticality of those services. The system manager will maintain contingency and disaster recovery plans to ensure this level of service availability and integrity.

12 FAM 642.4-2 Controlling Access to the Network

(TL:DS-51; 4-12-96)

a. System managers must restrict network access to only those users who have a demonstrated need for such access, and who have been authorized in writing by their supervisors for specific access rights. Additional information concerning methods of controlling access to the network is available from DS/CIS/IST.

b. The system manager will distribute a logon ID and password to all users in a secure manner, i.e., via STU, in person, or through other secure methods.

c. All users must sign a password receipt form. The system manager will retain a copy of this form, and as applicable, forward the original to the RCC system manager for archiving.

d. System managers must remove default user IDs that would permit unauthorized system access by network users.

e. The system manager must inform the appropriate RCC and NCC system managers, if existent, when a user no longer requires access to the network. The RCC and NCC system managers must then delete the individual user ID from the system access list and remove any assigned user access rights from data files and programs.

f. System managers must annually review the functional capabilities granted to all network systems and users. Functional capabilities must be based on the principle of least privilege.

g. System managers must delete a system from the system access list once the connection is no longer operationally necessary.

h. System managers must inform RCC and NCC system managers, if existent, prior to bringing additional end-points (network nodes) into operation.

i. System managers who are participants in a Department-wide network must inform the NCC system manager prior to adding or deleting area control center designations to or from their systems.

12 FAM 642.4-3 Pre-Logon Warning Message

(TL:DS-51; 4-12-96)

a. Where possible, system managers must ensure that users attempting to access a system are presented with a pre-logon warning message. The following warning message must be used:

"This computer is a Department of State computer system. It should be used for official U.S. Government work only; use by unauthorized persons, or for personal business, is prohibited and may constitute a violation of 18 U.S.C. 1030 and other Federal law. You have NO REASONABLE EXPECTATION OF PRIVACY while using this computer."

b. All data contained herein may be monitored, intercepted, recorded, read, copied, or captured in any manner by authorized personnel. System personnel or supervisors may give law enforcement officials any potential evidence of crime, fraud, or employee misconduct found on DOS computer systems. Furthermore, law enforcement officials may be authorized to access and collect evidence from this system:

"USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO THIS MONITORING.

IF YOU DO NOT CONSENT, LOG OUT NOW.

DO YOU AGREE TO ALL THE CONDITIONS STATED ABOVE? (Y/N)"

12 FAM 642.4-4 Connection to Other USG Agencies

(TL:DS-51; 4-12-96)

DS/CIS/IST and A/IM must approve the connection of a Department of State system to another U.S. Government agency system. The other agency must abide by the applicability statement found in section 12 FAM 613 .

12 FAM 642.4-5 Log and Record Keeping

(TL:DS-51; 4-12-96)

a. ISSOs must ensure that network-related logs and records are maintained for automated information systems networked to other systems or devices. Implementation instructions are provided by DS/CIS/IST.

b. The RCC and the NCC system managers must review their respective system network configuration information on an annual basis. This information must be retained for one year.

c. The ISSO will review the network based audit trail for potential security related incidents on a monthly basis. The ISSO will securely store audit information for six months from the date of the last log entry.

d. System managers must perform the following actions on an annual basis and forward a copy of the resulting information up the chain of command to the RCC or NCC system manager:

(1) System managers must document the purpose of each link to other systems including data processing, access to peripheral devices, messaging applications, distributed file sharing, distributed and remote execution of applications, electronic fund transfers, access to/for other agencies, etc.;

(2) System managers must identify and document the physical components supporting links from their systems to other systems including line speed, protocol, and safeguards implemented, e.g., encryption and procedural controls;

(3) System managers must identify all logically defined links and compare this information to the physical components documented in subparagraph (2) above. The system manager must resolve any discrepancies between logically defined links and physically defined links; and

(4) System managers must document the service.

12 FAM 642.4-6 Security Incident Procedures

(TL:DS-51; 4-12-96)

a. System managers must report all suspected or actual network compromises to the ISSO, DS/CIS/IST and, domestically, DS/DO. Notification must also be given up and down the chain of command (i.e., to local, regional and network control centers).

b. When a compromise is suspected or known, system managers must limit network operations in proportion to the perceived risks and potential damage.

12 FAM 642.4-7 System Maintenance

(TL:DS-51; 4-12-96)

a. Maintenance requirements found in subchapter 12 FAMs 620 and 630 must be followed as applicable.

b. For classified networks, system managers will permit employees of the local common carrier access only up to the point where their telecommunications equipment and lines terminate inside the facility, e.g., the frame room.

12 FAM 643 SYSTEMS IMPLEMENTATION

12 FAM 643.1 Distribution of Network Software

12 FAM 643.1-1 Software for Classified Networks

(TL:DS-51; 4-12-96)

a. The system manager ensures that all classified networks use only the Department approved and distributed version of network software.

b. The system manager may only install new releases, upgrades, or patches to the network software which are received from the Department. Software sent directly by a vendor or a vendor’s authorized distributor will not be installed on any network without prior A/IM approval.

c. Diplomatic courier pouch shipment of networking software for overseas use is required. Department of State or U.S. registered mail will be used for domestic distribution.

12 FAM 643.1-2 Software for Unclassified Networks

(TL:DS-51; 4-12-96)

a. The system manager must ensure that DS/CIS/IST is notified prior to installing network software which has never before been installed on a Department of State network.

b. System managers may install networking software received directly from the vendor.

12 FAM 643.2 Security Controls

12 FAM 643.2-1 Access Controls

(TL:DS-51; 4-12-96)

a. The system manager must enable all discretionary access controls for C-2 level networks. The system manager will restrict access to data, programs, etc., based on the identity of the users and/or the groups to which they belong.

b. The system manager will implement mandatory access control policies for multi-level AISs joined in a network. The system manager will restrict access to data, programs, etc., based on the sensitivity (as represented by a label) of the information contained in the data, program, etc. and the formal authorization (i.e., clearance) of users to access information of such sensitivity.

c. System managers must limit access to system software, utilities, and system services that could be used to gain unauthorized access to system data and software through network services. The system manager will prohibit users from accessing functions to which they have no defined need.

d. If the system provides mechanisms to exclude or include users based on method or location of entry, such as limiting users authorized to access the system via dial-up facilities or limiting users to/from specific devices, then the system manager must ensure that these mechanisms are enabled and maintained as appropriate.

e. Where possible, system managers must ensure that all connected systems access permissions default to “no access” for all access types definable for the connection, until a specific need has been established and approved. (Access types include read, write, modify, execute, delete, append, etc.) Once a need has been established, the principle of least privilege must be employed allowing only the level of access necessary for a user’s job duties.

f. The system manager must configure telecommunication service windows for attached systems for only those hours operationally required. After-hours access must not be configured unless a specific operational need has been identified and documented by the system manager and ISSO.

g. System managers must restrict node-hopping programs to those users who have a legitimate need to access remote systems. Where a need for intermediate logons by users to gain access to distant systems has been established, system managers must limit the functionality of these node-hopping programs in order to promote controlled access. These programs can be limited through the use of system-level security controls, locally developed procedures, or other mechanisms that control the selection of input parameter values.

h. System managers must ensure that users are limited to only one remote logon session at a time.

12 FAM 643.2-2 Protection and Placement of Incoming Files

(TL:DS-51; 4-12-96)

a. System managers must ensure that incoming files received through file transfer services are placed, protected, and given access rights which restrict users to only the information required to perform their official duties. Access privileges must be consistent with the separation of duties outlined in Chapter 12 FAM 500 for manual processes. Users must not be granted default permission to override system definitions.

b. Users will protect network data at the highest classification level of the network until a manual review of the data is conducted to determine its correct classification.

c. System managers must review the parameters specified under system network services that determine file types eligible and necessary for transfer between systems. As a default setting, the system manager will restrict the network connections so as to allow no exchange of traffic.

d. The system manager must ensure that only system staff are given direct access to the system file transfer software. Other users with an approved need to transfer files must access the transfer function indirectly through system level controls or locally developed procedures that restrict the file transfer capabilities to well defined parameters.

e. Where the capability exists, the system manager must establish a unique file transfer path for each connected system. File transfer paths may use logical designators. All file transfer paths must have defined data naming schemes, storage locations, file protection requirements, and an appropriate, non-blank “owner-of- record” identifier.

f. The system manager must ensure that users cannot by default modify the file transfer path which controls the storage and disposition of files.

g. The system manager will not allow file transfer to be used on networked systems when the capability to record user and originating system identification for data exchange activities does not exist.

12 FAM 643.2-3 Non-Repudiation

(TL:DS-51; 4-12-96)

a. Where required by the Department, the system manager will ensure that all parties in a transmission are provided with proof of delivery and are assured of the sender’s identity (non-repudiation). Neither party can deny having participated in all or part of the communications.

b. System managers will ensure that system-provided non-repudiation techniques are enabled for certification of electronic fund transfers (EFTs).

c. System managers will ensure that verification data recorded through non-repudiation techniques is protected from modification or unauthorized access or destruction.

12 FAM 643.2-4 Identification and Authentication (I&A)

(TL:DS-51; 4-12-96)

a. The system manager will utilize identification and authentication as the basis for correct network access control decisions.

b. System managers must ensure that each user is required to enter a unique user identifier (ID) and password prior to accessing and performing any actions for each new remote logon connection within the network. Network auto-logon features may not be used where user IDs and passwords are maintained on the system in script form (clear text executable instructions or parameter values) where the system does not require the user to enter the information for identification and authentication purposes.

12 FAM 643.2-5 Continuity of Operations

(TL:DS-51; 4-12-96)

a. System managers must implement procedures to ensure continuity of operations for networks. Additional information is available from DS/CIS/IST.

b. System managers must monitor network activity, gather usage statistics of links and devices and take action if established thresholds on central processing unit (CPU) usage, disk utilization or task activity are exceeded.

c. System managers must ensure that systems on the network have sufficient redundant control capabilities so as to reduce single points of failure, enhance reliability and survivability, and provide excess capacity. For example, the system manager may define a primary and secondary transmission path between systems within the network.

12 FAM 643.2-6 Encryption

(TL:DS-51; 4-12-96)

a. System managers are required to ensure that classified or unclassified sensitive data, transmitted over communication links that transit non-USG controlled space, is protected by the use of encryption as specified in subchapter 12 FAM 660.

b. The COMSEC custodian must follow all COMSEC requirements contained in subchapter 12 FAM 660 and S/KAG 1.

c. ISSOs must ensure that installed encryption devices are operational and appropriately keyed. Use of the bypass or plain-text mode is not permitted.

12 FAM 643.2-7 Traffic Flow Confidentiality

(TL:DS-51; 4-12-96)

Where deemed necessary by the Department, the system manager will ensure that traffic is padded to mask the frequency, length, and origin-destination patterns of communications between AISs.

12 FAM 643.2-8 Message Integrity

(TL:DS-51; 4-12-96)

System managers must ensure that selected countermeasures such as digital signatures, message authentication codes, etc., are enabled to prevent threats to network communications.

12 FAM 643.2-9 Virus Prevention

(TL:DS-51; 4-12-96)

System managers are required to implement virus prevention and detection programs for all systems connected to a Department network. Contact DS/CIS/IST for guidelines and procedures for computer virus detection, disinfection, prevention, and system restoration.

12 FAM 643.2-10 Logging and Monitoring

(TL:DS-51; 4-12-96)

a. Where available, the system manager will utilize network-based auditing to provide information for detection and analysis of security failures and intruder activities.

b. ISSOs must review network file transfer logs on a monthly basis. These logs must be reviewed for unsuccessful attempts at data exchanges, as well as for any actions outside of the routine file transfer activities that occur between the systems on the network. ISSOs will securely store these logs, either in automated or paper form, for six months from the date of the last entry. The ISSO will ensure that audit files stored in an automated fashion are purged from the AIS when they become outdated.

c. If the network operating system audit facilities provide the capability to capture the originating remote system connection identifier and the remote logon ID, then the system manager must ensure that these services are activated.

d. System managers must monitor tasks that exceed the network's defined thresholds.

e. System managers must ensure that no non-privileged user-level action, either deliberate or accidental, causes the network to be unavailable to other users.

12 FAM 643.2-11 Top Secret Control

(TL:DS-51; 4-12-96)

a. System managers will ensure that system-provided non-repudiation techniques have been enabled for send/receive transmissions of Top Secret data streams or objects.

b. For Top Secret systems, system managers will ensure that, where the capability has been provided, the destination system and the Top Secret Control Number (as referenced in section 12 FAM 539.2) are recorded with other required audit data.

12 FAM 644 TRANSMISSION FACILITY SECURITY

12 FAM 644.1 Modems, Multiplexors, Amplifiers, Repeaters, PBXs, Channel Banks, Boosters, and Concentrators

(TL:DS-51; 4-12-96)

Modems, multiplexors, amplifiers, repeaters, PBXs, channel banks, boosters, concentrators, etc., must be located so as to prevent accidental or malicious interruption of service or unauthorized use.

12 FAM 644.2 Protected Distribution Systems (PDSs)

(TL:DS-51; 4-12-96)

a. The system manager must follow all requirements in SKAL 500, CSM-27, and DTS/IS-1A for the construction of protected distribution systems for classified AISs.

b. If the area is not regularly monitored, or if visitors to the area are not under the direct observation of cleared U.S. Government employees, the system manager will ensure that unencrypted lines transmitting unclassified information, passing between facilities within a U.S. Government compound, are encased within a protected distribution system.

12 FAM 644.3 Data Encryption Standard (DES) Devices

(TL:DS-51; 4-12-96)

a. Data encryption standard (DES) equipment and its related support equipment, including COMSEC material, will be transported via diplomatic courier pouch.

b. The COMSEC custodian will be responsible for the initial receipt of the equipment and keying material. The keying material and KOI-18 will be hand-receipted on Form SF-153 to the system manager, who must possess cryptographic clearance for use. In the absence of the system manager’s clearance, the COMSEC custodian will have the responsibility to key the equipment.

c. The system manager for an unclassified system utilizing encryption may be an FSN; however only U.S. citizen employees may access the security functions key, crypto key, KOI-18 fill device, or other crypto accountable items. At some posts, there may be a requirement for designated FSN personnel to access the data communications functions key. Immediately after each use, the key must be secured in an approved safe.

d. U.S. Government direct-hire or contract personnel will mount the encryption devices on either desks or racks in the area where the unclassified computer equipment is located. During non-duty hours, the door to the room housing the data encryption devices must be secured with a DS-approved spin-dial or deadbolt lock. Access must be restricted to only authorized personnel. In instances where the tail circuit is in-house, the data link encryption device will be mounted in the CPU secondary tech control rack.

e. DES keying material, key loaders (KOI-18) and interface cable must be stored in an approved Class 6 safe. Only cleared U.S. citizens may have the combination to the security container.

f. The cryptographic keying material must be destroyed as soon as possible after supersession, but not later than twelve hours. A local destruction report (SF-153) should be prepared and filed. The destruction of the keying material must be witnessed. Approved destruction methods must be used, e.g., burning, shredding, or disintegration.

g. For applicable encryption devices, the system manager must place the SECURITY FUNCTIONS and DATA COMM FUNCTIONS locks in the LOCKOUT position (using the provided security keys) so that users are prevented from reconfiguring the encryption unit's operating parameters, loading or changing keys, checking which keys are in use, changing operating modes, testing the unit, viewing log displays, and viewing automatic key change parameters. The security keys must be stored in an approved Class 6 safe. Only cleared U.S. citizens may have the combination to the security container.

h. The COMSEC custodian will return defective DES encryption devices and associated keys to the Department via diplomatic courier pouch, attn: IM/SO/TO/MT. The COMSEC custodian will return defective KOI-18s via diplomatic courier pouch, attn: IM/SO/TO/INFS/CRYP.

i. The system manager will alert the COMSEC Custodian and ISSO if the internal tamper-proof switch on the encryption device is activated by unauthorized access to the inside of the unit. The ISSO will assist the RSO in the conduct of an investigation. Only an appropriately cleared U.S. citizen may reset the encryption device system parameters following a security incident.

12 FAM 645 MICROCOMPUTER SECURITY

12 FAM 645.1 Stand-Alone Government- Owned PCs Connected to Nongovernmental Systems

(TL:DS-51; 4-12-96)

a. System managers must ensure that PCs connected to nongovernmental systems are not simultaneously attached to Department systems.

b. System managers must ensure that data received from nongovernmental sources is not transferred to Departmental systems until the system manager performs a review of the data to ensure that it contains no malicious code.

c. Additional instructions relating to Internet type connections can be obtained from DS/CIS/IST.

12 FAM 645.2 Government-Owned PCs or Remote Workstations Installed in Private or Official Residences

(TL:DS-51; 4-12-96)

a. DS/CIS/IST must approve the placement and connectivity of government-owned PCs and remote workstations installed in private or official residences. Requesting officials must demonstrate a compelling operational requirement for the connection. Implementation instructions can be obtained from DS/CIS/IST.

b. The system manager may only connect off-site PCs or remote workstations to an unclassified host processor.

c. The ISSO will ensure that a Department-approved encryption device is installed between the off-site system and the host processor to prevent cleartext transmittal of information, especially user IDs and passwords.

12 FAM 645.3 Unclassified to Classified Connections

(TL:DS-51; 4-12-96)

The following security requirements apply for any systems identified and approved by the Department for one-way unclassified to classified connections:

(1) The system manager must ensure that the “Receive Data” Pin (Pin 3) has been removed from the unclassified processor end of the RS-232 cable, so that classified data cannot be received on the unclassified system;

(2) The system manager must ensure that the “Send Data” Pin (Pin 2) has been removed from the TERP end of the RS-232 cable, so that classified data cannot be transmitted to the unclassified system;

(3) The ISSO must ensure that only authorized individuals release telegrams from the unclassified system to a classified telecommunications processor;

(4) The Department has approved the Wang One Way Interface (WOWI) for transmissions from unclassified Wang systems to post classified telecommunications processors. The purpose of the one way connection is to enable users of the unclassified system to send unclassified telegrams electronically from the desktop to the telecommunications processor while inhibiting any flow of classified data from the telecommunications processor down to the unclassified processor. The Department may approve other connections of this type in the future;

(5) The ISSO must ensure that the placement and use of the workstation in the controlled access area (CAA) that is used for the WOWI connection is controlled in accordance with Chapter 600 and S/KAL 500 CSM-27.

12 FAM 645.4 Classified Connections to the TERP

(TL:DS-51; 4-12-96)

The system manager for the classified AIS will perform the following actions:

(1) The system manager must configure TERP user and workstation profiles so that TOP SECRET information can not be downloaded to a classified AIS;

(2) The system manager must configure TERP user and workstation profiles so that only those special distribution channels and captions required by individual users may be downloaded to a classified AIS from the TERP;

(3) The system manager must configure the TERP keyboard timeout option for a maximum of three minutes;

(4) The system manager must disable the connection between a classified AIS and the TERP after hours unless the Department has authorized unattended operation of the TERP;

(5) The system manager must ensure that departing classified AIS users are also removed from the TERP user profile;

(6) The ISSO must review the TERP security log containing classified AIS/TERP interactions when the daily journaling is done. The ISSO will securely store this log for six months from the date of the last entry. The ISSO will ensure that audit files stored in an automated fashion are purged from the TERP when they become outdated.

12 FAM 645.5 Electronic Mail (E-Mail)

(TL:DS-51; 4-12-96)

a. The ISSO should have read access to the user's mailbox to ensure that no messages contain classification levels higher than that allowed on the AIS.

b. The owner of the mailbox will allow access to other users based on a need to know. If access is needed on a temporary basis only, then that access should be revoked when no longer operationally required.

12 FAM 645.6 Facsimile (FAX) Gateways

(TL:DS-51; 4-12-96)

System managers must ensure that users are not allowed access to the FAX Gateway by default. Specific access to Fax Gateway menus, functions and data objects is to be granted only on an individual user basis.

12 FAM 645.7 Foreign Affairs Information System (FAIS) Software

(TL:DS-51; 4-12-96)

a. The system manager must configure the user profile within the electronic mail directory so that a sensitivity attribute relating to the authorized classification level is used to make network access decisions.

b. Users must assign appropriate classification levels to data objects.

c. Users must not enter data objects that exceed the approved classification level of the network.

d. The system manager must provide the user with the capability to assign the following advisory sensitivity attributes to messages:

(1) Special distribution captions;

(2) Channel distribution captions;

(3) Distribution captions;

(4) Captions;

(5) Tags;

(6) Terms;

(7) Geographical; and

(8) Functional bureau responsibilities.

e. The user must assign sensitivity attributes where applicable.

f. Users must assign the following advisory attributes:

(1) Data author/owner;

(2) Drafting date; and

(3) Top Secret control number.

g. System managers must implement the system security controls identified in FAIS Network Security Criteria and additional implementation requirements promulgated by A/IM.

12 FAM 646 DOMESTIC AND OVERSEAS AUTOMATED INFORMATION SYSTEMS CONNECTIVITY

12 FAM 646.1 General

(TL:DS-51; 4-12-96)

a. These requirements ensure that the use of telecommunication technologies does not result in degradation of the security posture of the Department's automated information systems (AIS).

b. The decision whether or not to connect the Department's systems is based upon their mode of operation, level of trust of the operating system and/or security subsystem, and the classification level of processing.

12 FAM 646.2 Mode of Operation for Automated Information Systems

12 FAM 646.2-1 System-High Operations

(TL:DS-51; 4-12-96)

An AIS is operating in a system-high mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A valid personnel security clearance for all information on the AIS;

(2) Formal access approval for all information stored and/or processed (including all compartments, subcompartments, and/or special access programs); and

(3) A valid need-to-know for at least some of the information contained on the AIS.

12 FAM 646.2-2 Multi-Level Operations

(TL:DS-51; 4-12-96)

An AIS is operating in a multi-level mode when all of the following statements are satisfied concerning the users with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:

(1) Some do not have a valid personnel security clearance for all information on the AIS;

(2) All have the proper security clearance (for classified information) and the appropriate formal access approval for that information to which they are to have access; and

(3) All have a valid need-to-know for that information to which they are to have access.

12 FAM 646.2-3 Dedicated Operations

(TL:DS-51; 4-12-96)

An AIS is operating in a dedicated mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A valid personnel security clearance for all information on the AIS;

(2) Formal access approval for all information stored and/or processed (including all compartments, subcompartments, and/or special access programs); and

(3) A valid need-to-know for all of the information contained on the AIS.

12 FAM 646.3 Level of Trust for Automated Information Systems

12 FAM 646.3-1 C-2 Level of Trust for Classified AISs

(TL:DS-51; 4-12-96)

The Trusted Computer System Evaluation Criteria (TCSEC) requires that C-2 systems listed in the EPL provide controlled access protection for all information on the AIS. It also requires identification and authentication, auditing of security relevant events, discretionary access controls, and object reuse. (Note: section 12 FAM 641.3-2 contains alternative security requirements for personal computers.)

12 FAM 646.3-2 C-2 Functionality for Unclassified Systems

(TL:DS-51; 4-12-96)

Documentation concerning an operating system’s controlled access protection must be made available for review by appropriate security personnel.

12 FAM 646.3-3 B and A Levels of Trust

(TL:DS-51; 4-12-96)

The required level of trust is directly related to the difference between the clearance of the users and the classification of the data on the system. System developers and acquisition authorities should contact DS/CIS/IST for more information.

12 FAM 646.4 Methodology for Connecting Systems Based on the Operating Mode, Level of Trust, and Classification

(TL:DS-51; 4-12-96)

a. The Department does encourage upgrading existing operating systems, application software, and network software to provide C-2 functionality whenever possible. Connections to distributed AIS fielded before October 1, 1995 will be based upon mode of operation and classification level, not level of trust.

b. One-way communication links between unclassified and classified systems, e.g., WOWI, have been approved by the Department based on acceptable software controls and are exempted from this policy. Implementation instructions for approved one-way connections can be obtained from DS/CIS/IST.

c. The connection of an unclassified DOS distributed system to a non-governmental system presents additional vulnerabilities, and may only be accomplished via a DS-approved firewall. Contact DS/CIS/IST for implementation instructions.

d. DS/CIS/IST is currently developing policy which will approve the connection of multi-level AISs, having B or A levels of trust, in a network.

12 FAM 647 ADMINISTRATIVE SECURITY

(TL:DS-51; 4-12-96)

a. In a hierarchical network, local system managers and information system security officers (ISSOs) report up the chain of command to regional and then worldwide network staff, as applicable. In a network where all connections are equal, individual system managers and ISSOs report directly to a network control center. In both cases, one system manager and one ISSO will exercise authority over the entire network.

b. Pre-logon warning message: Warning messages are used to deter unauthorized use, increase computer security awareness, and provide a legal basis for prosecuting unauthorized access.

12 FAM 648 SYSTEMS IMPLEMENTATION — SECURITY CONTROLS

12 FAM 648.1 Access Controls

(TL:DS-51; 4-12-96)

Discretionary access controls for C-2 level networks are discretionary in the sense that a user with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other user (unless restrained by mandatory access control).

12 FAM 648.2 Non-Repudiation

(TL:DS-51; 4-12-96)

Non-repudiation services can be provided through the use of public key encryption techniques that create electronic signatures or other techniques.

12 FAM 648.3 Encryption

(TL:DS-51; 4-12-96)

a. Encryption on links between unclassified, non-sensitive stand-alone DOS computers and non-government systems is not required.

b. The Department does not require encryption on Foreign Affairs agency tail-circuits (i.e., local systems circuits servicing Foreign Affairs agencies in a limited geographical area) which:

(1) Utilize the unclassified Department of State telecommunications facility distribution services only; and

(2) Have no connection to a Department of State computer system, e.g., VS or LAN.

12 FAM 648.4 Logging and Monitoring

(TL:DS-51; 4-12-96)

Network operating system level audit controls designed to capture data at the point of entry or point of departure must be invoked by the system manager where they are available. Services provided to capture identification and authentication information, changes to access control lists, use of sensitive files, and modifications made to ENCRYPT1 software must be activated.

12 FAM 649 TRANSMISSION FACILITIES SECURITY

12 FAM 649.1 Encryption

(TL:DS-51; 4-12-96)

System managers must notify DTS-PO of the need for encryption so that encryption devices can be provided and made operational prior to the activation of the link.

12 FAM 649.2 Black KG-84s

(TL:DS-51; 4-12-96)

a. The ISSO may request a black KG-84 to encrypt unclassified transmissions.

b. The Department (A/IM) will apply black paint to the exterior top of the KG-84 to signify that this device will be located in an area where Foreign Service nationals have unescorted access. The black KG-84 can never be used in a controlled access area.

c. The KG-84 and its related support equipment, including COMSEC material, will be transported via diplomatic courier pouch or by Defense courier service.

d. The COMSEC custodian will be responsible for the initial receipt of the equipment and keying material. The keying material will be hand receipted on Form SF-153 to the system manager, who must possess cryptographic clearance for use. In the absence of the system manager’s clearance, the COMSEC custodian will have the responsibility to key the equipment at the UNCLASSIFIED level.

e. Technically qualified U.S. personnel possessing cryptographic clearance will install the KG-84 device on either desks or racks in the area where the unclassified computer equipment is located. This area must be locked during non-duty hours, and be under the operational control of a U.S. citizen. Offices with doors that have key locks are acceptable.

f. The system manager will note that both keyed and unkeyed black KG-84s are designated as unclassified controlled cryptographic items (CCIs) and must be protected as high value COMSEC accountable items.